IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	Criminal No. 1:15-CR-00309
	:	
v.	:	(Chief Judge Conner)
	:	
JALIL IBN AMEER AZIZ	:	(Electronically Filed)

BRIEF IN SUPPORT OF MOTION FOR NOTICE AND DISCLOSURE OF FISA-RELATED SURVEILLANCE AND TO SUPPRESS THE FRUITS OR DERIVATIVES OF ELECTRONIC SURVEILLANCE AND ANY OTHER MEANS OF COLLECTION CONDUCTED PURSUANT TO FISA OR OTHER "CONFIDENTIAL" FOREIGN INTELLIGENCE GATHERING OR ANY PARALLEL CONSTRUCTION OR "SCRUBBING" ACTIVITIES

Thomas A. Thornton, Esquire
Attorney ID# 44208
Federal Public Defender's Office
100 Chestnut Street, Suite 306
Harrisburg, PA 17101
Tel. No. 717-782-2237
Fax No. 717-782-3881
tom_thornton@fd.org

Table of Contents

Table of Authorities

I. Introduction

The government has filed notice that it intends "to offer into evidence, or otherwise use or disclose in any proceedings in this matter, information obtained and derived from electronic surveillance conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 ("FISA"), as amended, 50 U.S.C. §§ 1801-1812 and 1821-1829." (Doc # 21) In the normal criminal case, the government would be required to provide the bases for its surveillance and searches so that defense counsel could then file appropriate motions for the Court to rule on and determine whether the government violated the law during its investigation of Jalil Aziz, and that it should therefore be barred from introducing any tainted evidence against him. However, the specter of national security concerns triggered by FISA put such basic information beyond the reach of counsel—no matter how improper FISA surveillance could be in this case.

Discovery tendered by the government has revealed voluminous electronic communications, and other online activity involving Jalil Aziz. These electronic communications include emails from several email accounts and is believed to include to postings on various online forums which are visited by other Americans on a daily basis. While it is unclear when the government's use of FISA surveillance began as such details have not been disclosed, the complaint and discovery indicate early implementation of that surveillance. There is also

evidence that the government surreptitiously entered the Aziz home and placed surveillance devices inside while searching the residence without notice to the Aziz family.

Thus, while it is unclear precisely which electronic communications or other evidence was collected pursuant to FISA and over what exact time period, as discussed in detail below, the numerous e-mails, online activity, and other electronic information that the government presumably obtained pursuant to FISA or other foreign intelligence must be suppressed because the surveillance and/or collection violated the provisions of FISA as well as the principles of the First, Fourth, Fifth, and Sixth Amendments.

As discussed in detail below, this brief identifies the following independent and alternative bases for suppression or exclusion:

a) the FISA applications for electronic surveillance of Jalil Aziz's e-mail accounts may fail to establish probable cause that he was "an agent of a foreign power";

b) those FISA applications may contain intentional or reckless material falsehoods or omissions, and therefore may violate the Fourth Amendment principles identified by the Supreme Court in *Franks v. Delaware*, 438 U.S. 154 (1978)

c) the primary purpose of the electronic surveillance was to obtain evidence of domestic criminal activity and not foreign intelligence information—or, conversely, capturing foreign intelligence information was not a "significant" purpose of the FISA surveillance[1];

d) the FISA surveillance may have been based impermissibly on activity protected by the First Amendment;

e) the government may not have made the required certifications in the FISA applications, or may have failed to obtain necessary extensions of prior FISA orders, or continued the FISA surveillance after any basis for such initial surveillance was no longer valid;

f) the government may not have established or abided by the appropriate minimization procedures required by FISA;

[1] As discussed in greater detail in Section VI, infra, effective October 26, 2001, Congress amended §1804(a)(6)(B) through the USA PATRIOT Act to require government certification only that "a significant purpose"—rather than" the purpose"—of the surveillance is to obtain foreign intelligence information. (Emphasis added). In May, 2002, the Foreign Intelligence Surveillance Court of Review, a federal court empowered to review the denial of a FISA application by the FISA Court, issued its first ever opinion in its 24-year history, in which, in dicta, it endorsed the "significant" purpose standard's constitutionality. See *In re Sealed Case,* 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002). *See also United States v. Abu Jihaad*, 630 F.3d 102, 120 (2d Cir. 2010), and cases cited therein. *But see Mayfield v. United States*, 504 F. Supp.2d 1023 (D. Ore. 2007). While counsel recognizes that the only Circuit decisions on this point are adverse, he nevertheless intends to preserve a challenge to the constitutionality of this amendment to the extent that the post-October 26, 2001, FISA-generated interceptions, or any evidence or information derived therefrom, are introduced against him in this case.

g) the government may have violated other provisions of FISA and/or the First and/or Fourth Amendments in manners unknown to Jalil Aziz; and,

h) Jalil Aziz's right to due process and effective assistance of counsel as guaranteed by the Fifth and Sixth Amendments would be abridged as a result of the lack of notice and disclosure.

However, because defense counsel has not been provided with the underlying applications for the pertinent FISA warrants, this brief can only outline the possible bases for suppression or exclusion for the Court to examine and consider. Counsel therefore respectfully requests that the Court:

a) review all applications for electronic surveillance of the defendant conducted pursuant to FISA;

b) order the disclosure of the applications for the FISA warrants to Defendant's counsel pursuant to an appropriate protective order;

c) conduct an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978); and, thereafter suppress any evidence, derived from illegally authorized or implemented FISA electronic surveillance; or,

d) preclude the government from using any FISA evidence or derivatives therefrom.

II. The History, Purposes, and Provisions of FISA.

FISA, 50 U.S.C. §1801, et seq., was enacted in 1978 in the wake of domestic surveillance abuses by federal law enforcement agencies as catalogued in Congressional Committee and Presidential Commission Reports.[2] The statute was designed to provide a codified framework for foreign intelligence gathering within the confines of the United States in response to civil liberties concerns and the gap in the law noted by the Supreme Court in *United States v. United States District Court (Keith, J.)*, 407 U.S. 297, 308-09 (1972).

Through FISA, Congress attempted to limit the propensity of the Executive Branch to engage in abusive or politically-motivated surveillance. FISA constituted Congress' attempt to balance the "competing demands of the President's constitutional powers to gather intelligence deemed necessary to the security of the Nation, and the requirements of the Fourth Amendment." H.R. Rep. No. 95-1283, at 15. As a result, FISA's provisions represented a compromise

[2] See, e.g., FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, S. Rep. No. 94-755, 94th Cong., 2d Sess. (1976); Commission on CIA Activities Within the United States, Report to the President (1975) (commonly referred to as the "Rockefeller Commission Report"). See also *United States v. Belfield*, 692 F.2d 141, 145 (D.C. Cir. 1982) ("[r]esponding to post- Watergate concerns about the Executive's use of warrantless electronic surveillance, Congress, with the support of the Justice Department, acted in 1978 to establish a regularized procedure for use in the foreign intelligence and counterintelligence field").

between civil libertarians seeking preservation of Fourth Amendment and privacy rights, and law enforcement agencies citing the need for monitoring agents of a foreign power operating in the United States. *See In re Kevork*, 788 F.2d 566, 569 (9th Cir. 1986) (FISA "was enacted in 1978 to establish procedures for the use of electronic surveillance in gathering foreign intelligence information. . . . The Act was intended to strike a sound balance between the need for such surveillance and the protection of civil liberties") (quotation omitted). Since its inception, FISA's constitutionality has been upheld without exception.[3]

Important differences exist between the standards for a FISA warrant and that issued under the Fourth Amendment and/or Title III of the U.S. Criminal Code. The "probable cause" required under FISA is merely that the target qualifies as an "agent of a foreign power,"[4] and not that a crime has been, or is being, committed, but rather that the "agent of a foreign power" will use the electronic device subject to electronic surveillance, or owns, possesses, uses, or is in the premises to be searched. [5]

---

[3] See, e.g., *United States v. Abu Jihaad*, 630 F.3d 102 (2d Cir. 2010); *United States v.Johnson*, 952 F.2d 565, 572 (1st Cir. 1991); *United States v. Pelton*, 835 F.2d 1067 (4th Cir 1987); *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984); *United States v. Megahey*, 553 F.Supp. 1180 (E.D.N.Y. 1982), aff'd, 729 F.2d 1444 (1983) (Table).

[4] See 50 U.S.C. §§1801(b).

[5] See 50 U.S.C. §§1805(a)(3) & 1824(a)(3).

In that context, FISA establishes procedures for surveillance of foreign intelligence targets, pursuant to which a federal officer acting through the Attorney General may obtain judicial approval for conducting electronic surveillance for foreign intelligence purposes. The FISA statute created a special FISA Court—the Foreign Intelligence Surveillance Court (hereinafter "FISC")[6]—to which the Attorney General must apply for orders approving electronic surveillance of a foreign power, or an agent of a foreign power, for the purpose of obtaining foreign intelligence information. *See* 50 U.S.C. §§1802(b), 1803 & 1804.8 The FISC is a unique court, as it operates in secret with only the government permitted to appear before it.

Thus, as the Ninth Circuit explained in *United States v. Cavanagh*, 807 F.2d 787 (9th Cir.1987), "[w]ith important exceptions not pertinent here, FISA requires judicial approval before the government engages in any electronic surveillance for foreign intelligence purposes." *Id*. at 788. FISA also requires that any application to the FISA Court be made under oath by a federal officer and contain certain information and certifications found in §1804, which, in summary, are as follows:

[6] The FISC consists of eleven judges (previously seven prior to amendments adopted as part of the USA PATRIOT Act) who individually hear government applications. *See* 50 U.S.C. §1803.

(1) the FISA application must provide the identity of the federal officer making the application. §1804(a)(1);

(2) the FISA application must identify or describe the target. §1804(a)(2);

(3) the FISA application must contain "a statement of the facts and circumstances relied upon by the applicant to justify his belief that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power and each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used by a foreign power or an agent of a foreign power[.]" §1804(a)(3). *See United States v. Posey*, 864 F.2d 1487, 1490 (9th Cir. 1989). FISA defines the term "foreign power," in pertinent part as "a group engaged in international terrorism or activities in preparation therefor." §1801(a)(4);

(4) the application to the FISC must provide a "statement of the proposed minimization procedures." §1804(a)(4);

(5) the FISA application must include a "description of the nature of the information sought and the type of communications or activities to be subjected to surveillance." §1804(a)(5). Thus, FISA appears to require that both the information sought and the communications subject to surveillance would

have to relate directly to activities involving both an agent of a foreign power and international terrorism as defined in FISA;[7]

(6) the FISA application must include certain "certifications," enumerated in §1804(a)(6)(A)-(E), and made by designated government officials, that:

(A) the certifying official deems the information sought to be foreign intelligence information;

(B) the purpose of the surveillance is to obtain foreign intelligence information;

(C) such information cannot reasonably be obtained by normal investigative techniques;

(D) designates the type of foreign intelligence information being sought according to the categories described in" §1801(e); and

(E) includes a statement of the basis for the certification that –

[7] Section 1801(c) defines "international terrorism" as follows:
(c)"International terrorism" means activities that –
(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
(2) appear to be intended –
(A) to intimidate or coerce a civilian population;
(B) to influence the policy of a government by intimidation or coercion; or
(C) to affect the conduct of a government by assassination or kidnapping; and
(3) occur totally outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques.

(7) the FISA application must contain a statement of the means by which surveillance will be effected and a statement whether physical entry is required to effect the surveillance. §1804(a)(7);

(8) the FISA application must contain a statement of facts listing all previous related FISA applications made to any FISC judge, and action taken on each previous application. §1804(a)(8); and

(9) the FISA application must specify the period of time for which the electronic surveillance is required to be maintained. §1804(a)(9).

In addition, the Attorney General must personally review the application and determine whether it satisfies the criteria and requirements set forth in FISA. §1804(d); see §1805(a)(1). Regarding the judicial component of the FISA process, in considering an application for electronic surveillance pursuant to FISA, the Court should reject the application unless the application meets the following criteria sufficient to permit the Court to make the requisite findings under §1805(a):

(i) that the application was made by a federal officer and approved by the Attorney General;

(ii) that there exists probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . and . . . each of the facilities or places at which the electronic surveillance is directed is being used or is about to be used by a foreign power or agent of a foreign power[;]"

(iii) that the proposed minimization procedures meet the definition of minimization procedures under §1801(h); and,

(iv) that the application contains all required statements and certifications. Also, in accordance with §1805(a)(4), if a target is a "United States person," the FISC must determine whether the "certifications" under §1804(a)(6)(E)—namely that the information sought is "the type of foreign intelligence information designated," and the information "cannot reasonably be obtained by normal investigative techniques"—are "not clearly erroneous." In addition, §1805(a)(2)(A) provides "that no United States person may be considered a foreign power . . . solely upon the basis of activities protected by the first amendment." As a natural born U.S. citizen, Jalil Aziz qualifies as a "United States person" under § 1801(i).

Critical to the operation of FISA and its application in this case are the definitions related to "foreign power" set forth in 50 U.S.C. § 1801. A "foreign power" is defined in § 1801(a) to include foreign governments, groups they control, and groups engaged in terrorism. An "Agent of a foreign power" is defined as any person who:

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or,

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any

person to engage in activities described in subparagraph (A), (B), or (C). 50 U.S.C. §1801(b)(2). [8]

Orders authorizing FISA wiretaps are issued for certain specified periods of time, but can be extended pursuant to additional applications. §§1805(d)(1) & (2). FISA authorizes any "aggrieved person" to move to suppress evidence obtained or derived from an electronic surveillance on the grounds that "the information was unlawfully acquired" or "the surveillance was not made in conformity with an order of authorization or approval." §§1806(e)(1) & (2); 1825(f). FISA defines "aggrieved person" as "a person who is the target of electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." §1801(k). FISA permits evidence generated in intelligence investigations to be used in criminal prosecutions. §§1806(b) & 1825(c). Certainly Jalil Aziz is an "aggrieved person" who should have the right to suppression.

III. Jalil Aziz's Challenges to the FISA Electronic Surveillance In This Case.

Counsel cannot address any specific content or details of any of the FISA applications in this case because those applications have not been provided to

[8] Section 1801(b)(1) defines an "Agent of a foreign power" by a series of acts done by someone who is any person "other than a United States person" that are much broader than those set forth in subsection (b)(2) and quoted above, which are applicable to "United States persons."

counsel. While aggrieved criminal defendants, like Mr. Aziz, can move to suppress FISA-generated evidence, §1806(f) provides that if the Attorney General files an affidavit that "disclosure or an adversary hearing would harm the national security of the United States," the court deciding the motion must consider the application and order for electronic surveillance in camera to determine whether the surveillance was conducted lawfully. As addressed in more detail below, § 1806(f) provides:

> [i]n making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

Alternatively, §1806(g) provides that "[i]f the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." Here, although the defense has not been notified whether the Attorney General has yet submitted an affidavit under §1806(f), it is assumed for purposes of this motion that the government has made such a filing, and the arguments presented below in favor of suppression are made in response to that filing and the government's position that ex parte proceedings are necessary. Thus, the grounds for relief set forth below represent defense counsel's best estimation of the deficiencies in the FISA electronic surveillance in this case.

It goes without saying that the lack of access to the underlying FISA materials presents a significant impediment to any defendant's capacity to challenge FISA surveillance with much particularity. As the Fourth Circuit recognized in a closely analogous context, (discerning what exculpatory evidence a witness solely within the government's control, and to whom the defense is denied access, can provide) when a defendant is deprived of such access, the burden to be specific with respect to the material in question must be relaxed accordingly. *See United States v. Moussaoui*, 382 F.3d 453, 472 (4th Cir. 2004), citing *United States v. Valenzuela-Bernal*, 458 U.S. 858, 870-71, 873 (1982).

A. The FISA Applications Failed to Establish the Requisite Probable Cause.

1. The Elements of Probable Cause under FISA.

Before authorizing FISA surveillance, the FISA Court must find, inter alia, probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power." §1805(a)(2)(A). The Supreme Court has reiterated the long-standing rule that criminal probable cause requires "a reasonable ground for belief of guilt," and that "the belief of guilt must be particularized with respect to the person to be searched or seized." *Maryland v. Pringle*, 540 U.S. 366, 371 (2003). Under FISA, though, unlike a traditional

warrant, the probable cause standard is directed not at the target's alleged commission of a crime, but at the target's alleged status as "a foreign power or an agent of a foreign power."

2. The "Agent of a Foreign Power" Requirement.

Consequently, this Court must initially determine, with respect to each application for FISA electronic surveillance of Jalil Aziz, whether the application established a reasonable, particularized ground for belief that Jalil Aziz qualified as an "agent of a foreign power." 1805(a)(2)(A) & 1801(b)(2)(C) & (E). As set forth above, FISA provides several definitions for an "agent of a foreign power," and multiple definitions for a "foreign power." These definitions include a requirement that a person's activities are or may be in violation of the criminal laws of the United States. 50 U.S.C. §§ 1801(b)(2)(A) and (B), (c)(1), and (d). The need to establish a relationship to criminal activity for United States persons, such as Jalil Aziz, is made clear by the legislative history of FISA. H.R. Rep. 95-1283, Pt. 1 at 36, 95th Cong., 2d Sess. 21 (1978). The only decision issued by the Foreign Intelligence Court of Review ("FISCR"), which is the appellate court for the FISC, underscored this point when it noted that the definition of agent of a foreign power for United States persons "is closely tied to criminal activity." *In re Sealed Case*, 310 F.3d 717, 738 (FISA Ct. Rev. 2002).

Here, absent an opportunity to review the applications or any of the surveillance orders at issue, defense counsel cannot specify whether the allegations asserting that Jalil Aziz was an "agent of a foreign power" were sufficient to satisfy FISA. Because Jalil Aziz is an American citizen, any warrant should have been issued under § 1801(b)(2). Most of the authority for a warrant against a United States person is obviously inapplicable to this case. There is no suggestion that Jalil Aziz engaged in clandestine intelligence gathering (§ 1801(b)(2)(A)), acted under the direction of an intelligence network of a foreign power (§1801(b)(2)(B)), that he knowingly engaged in sabotage or international terrorism on behalf of a foreign power (§1801(b)(2)(C)), that he entered the United States under a false or fraudulent identity (§1801(b)(2)(D)), or that he aided or abetted or conspired in any such activity (§ 1801(b)(2)(E)).

Indeed, in reviewing FISA's definitions of "agent of a foreign power" under § 1801(b)(2), it is difficult to comprehend which was most likely utilized for Jalil Aziz, an natural born American of natural born citizen parents whose internet activities led him to websites and material that the government appears to deem inherently dangerous and to justify electronic surveillance. Yet such activity, even if questionable to the government, certainly does not qualify under FISA's definitions and render Jalil Aziz an "agent of a foreign power," particularly given the First Amendment protections afforded by §1805(a)(2)(A). Thus, it appears that

it would be quite difficult, if not impossible, for a FISA application to set forth the requisite evidence to establish probable cause that Jalil Aziz was an "agent of foreign power."

Moreover, because FISA requires proof of criminal activity to support surveillance or search of a United States person, significant questions may also arise involving the interplay between the FISA standard and the long-standing rules that probable cause requires "a reasonable ground for belief of guilt" and "the belief of guilt must be particularized with respect to the person searched or seized." *See Maryland v. Pringle*, 540 US. 366, 371 (2003). Thus, in addition to providing grounds for suppression, these points illustrate why the involvement of defense counsel will be necessary to counter arguments the government likely made in support of the validity of any FISA application or warrant.

3. The Nature and Origins of the Information in the FISA Applications.

Again, unlike the case with traditional warrants, non-disclosure of the FISA applications denies the defense the ability to contest the accuracy and/or reliability of the underlying information used to satisfy FISA's version of probable cause. As a result, absent such disclosure Jalil Aziz can request only that the Court review the FISA applications cognizant of certain factors and principles.

a) The Limits of "Raw Intelligence."

For example, foreign intelligence information is often in the form of "raw intelligence," and is not vetted in the manner typical of the information law enforcement agents' supply in ordinary warrant applications, i.e., that the information emanated from a source that was reliable and/or had a verifiable track record, or was independently corroborated. Such FISA raw intelligence is often not attributed to any specific source, and its genesis can be multiple-level hearsay, rumor, surmise, and speculation. Also, the motivation driving sources of raw intelligence to impart information is usually not nearly as transparent as in conventional criminal justice circumstances. As a result, the dangers of deception and disinformation are significantly enhanced.

b). Illegitimate and/or Illegal Sources of Information.

There is also the danger that the information in FISA applications, whether or not attributed to a particular source, was generated by illegal means such as warrantless wiretapping or constitutionally infirm FISA amendments that have yet to be challenged in criminal cases. In that context, the government should be compelled to disclose whether information in the FISA applications, or which was used to obtain information that appears in the applications, or was used in the investigation

in this case in any fashion, originated from such illegitimate means. *See Gelbard v. United States*, 408 U.S. 41 (1972) (in prosecution for contempt for refusal to testify, grand jury witness entitled to invoke as a defense statutory bar against use of evidence obtained via illegal wiretap as basis for questions in grand jury).

(1) The Warrantless Terrorist Surveillance Program.

For example, the government should be required to disclose whether any of Defendant's communications were intercepted pursuant to the Terrorist Surveillance Program (hereinafter "TSP"), a warrantless wiretapping program instituted in 2001. See *In re National Security Agency Telecommunications Records Litigation* (pertaining to: *Al-Haramain Islamic Foundation, Inc. v.Bush*), 451 F. Supp.2d 1215 (D. Ore. 2006), rev'd and remanded, 507 F.3d 1190 (9th Cir. 2007), on remand to Northern District of California, 564 F. Supp.2d 1109 (N.D. Cal. 2008), after remand, 700 F. Supp.2d 1182 (N.D. Cal. 2010). *See also ACLU v. National Security Agency*, 438 F.Supp. 2d 754 (E.D. Mich.2006), rev'd on standing grounds, 493 F.3d 644 (6th Cir. 2007). The government should further be compelled to disclose whether any communications intercepted pursuant to the TSP–whether or not Jalil Aziz was a party–contributed

to the FISA applications or the search warrant applications or to the investigation of this case in any manner.

(2) Surveillance Pursuant to the FAA.

The Court should also examine whether any portion of the FISA electronic surveillance was requested and conducted pursuant to the authority provided in 50 U.S.C. §1881a, enacted in 2008 as part of the FISA Amendments Act of 2008, Pub. L. No. 110-261 (2008) (hereinafter "FAA"), or whether any information in the FISA applications was the product of surveillance authorized under the FAA. The FAA provisions raise constitutional issues different from those implicated by the pre-existing FISA provisions. The government should not have any legitimate interest in obscuring the authority pursuant to which it conducted FISA surveillance herein; indeed, refusal by the government to so disclose would deny Jalil Aziz a fair trial by depriving him of due process, effective assistance of counsel, and any meaningful opportunity to contest the acquisition and admissibility of evidence that may have been obtained unlawfully.

(3) Surveillance Under Executive Order 12,333.

Executive Order 12,333 serves as the "primary source" of the NSA's foreign intelligence- gathering authority and governs most surveillance conducted abroad. [9] According to the NSA's own documents, the agency "conducts the majority of its [signals intelligence] activities solely pursuant to" E.O. 12,333.[10] Over the past three years, it has grown increasingly clear that the scale of the government's surveillance under E.O. 12,333 is vast – and that the government uses this information when investigating individuals here in the United States.[11] Under this authority, the NSA collects both content – such as phone calls, emails, and text messages – and so-called "metadata," like phone records, records of internet activity, and location information.

Surveillance programs operated under E.O. 12,333 have never been reviewed by any court. Moreover, these programs are not

[9] See NSA Overview of Signals Intelligence Authorities, p. 4 (Jan. 8, 2007), http://bit.ly/1ruKbBk; see also 3 C.F.R. § 202, 210–12 (1981), reprinted as amended, note following 50 U.S.C. § 401, pp. 543, 547–48.

[10] NSA Legal Fact Sheet: Executive Order 12,333, at 1 (Jun. 19, 2013), http://bit.ly/1CG9EtT.

[11] See generally Amos Toh, Faiza Patel, & Elizabeth Goitein, Overseas Surveillance in an Interconnected World, Brennan Center (Mar. 16, 2016), http://bit.ly/1UfSdMW; Two Sets of Rules for Surveillance, Within U.S. and on Foreign Soil, N.Y. Times (Aug. 13, 2014), http://nyti.ms/1u2juDt (chart describing uses of E.O. 12,333 surveillance).

governed by any statute, including FISA, and, as the chair of the Senate Intelligence Committee has conceded, they are not overseen in any meaningful way by Congress.[12] Instead, E.O. 12,333 surveillance is conducted entirely under Executive Branch authority, on the basis of a presidential directive first issued by President Reagan in 1981. As a result, there are few statutory or practical constraints on the government's use of this authority, even when it sweeps in huge quantities of Americans' data overseas. As a former State Department official recently wrote, "Executive Order 12,333 contains nothing to prevent the NSA from collecting and storing all such communications – content as well as metadata – provided that such collection occurs outside the United States in the course of a lawful foreign intelligence investigation. No warrant or court approval is required, and such collection need never be reported to Congress."[13]

Based on the public record, the government rarely provides notice to criminal defendants when its investigation has relied upon surveillance conducted under E.O. 12,333. In fact, according to

[12] See Ali Watkins, Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued, McClatchy, Nov. 21, 2013, http://bit.ly/1lCXFsC.

[13] See, e.g., John Napier Tye, Op-Ed, Meet Executive Order 12,333: The Reagan Rule That Lets the NSA Spy on Americans, Wash. Post (July 18, 2014), http://wapo.st/1wPuzv2.

unnamed government officials, the Justice Department believes that it has no legal obligation to provide notice to defendants, at least where its evidence is only "derived" – as opposed to obtained directly – from E.O. 12,333 surveillance.[14]

To be clear, if any part of the FISA surveillance was conducted pursuant to the FAA, TSP or E.O. 12, 333, Jalil Aziz intends to move to suppress any interceptions, and their fruit, on several grounds, including those summarized here:

- FAA, TSP, and E.O. 12, 333 violate several Fourth Amendment principles, including (a) the prohibition on general warrants; (b) the requirement that searches be reasonable; (c) the requirement that warrants be issued only upon prior judicial authorization based on an individualized determination of probable cause, and particularizing the place to be searched and the items to be seized; (d) the requirement of meaningful, court-supervised minimization; (e) the

[14] See Charlie Savage, Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide, N.Y. Times (Aug. 13, 2014), http://nyti.ms/1wPw6l0.

requirement that the electronic surveillance be of limited and precise duration; and (f) that the electronic surveillance's primary purpose be to collect foreign intelligence information;

- FAA, TSP, and E.O. 12, 333 surveillance violate the First Amendment because of the chilling effect it has on protected speech and association; and
- FAA, TSP, and E.O. 12, 333 surveillance violate Article III's separation of powers because the FAA requires the judicial branch to issue rulings absent any case or controversy, and to rule on the constitutionality of a government surveillance in the abstract, leaving determination of individualized monitoring exclusively to the Executive branch. Accordingly, the Court should examine the nature, genesis, and provenance of the information in the FISA application, and compel the government to disclose whether any such information was the product of warrantless electronic surveillance (either via the TSP, E.O.

12, 333 or any other similar program), or of such surveillance authorized pursuant to the FAA (§1881a).

4. FISA's Prohibition of Basing Probable Cause Solely On a "United States Person's" Protected First Amendment Activity.

FISA includes an additional restriction for electronic surveillance of a "United States person," as it prohibits finding probable cause for such a target based solely upon First Amendment activities. In making that probable cause determination, the statute directs "[t]hat no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment." §1805(a)(2)(A). Accordingly, if the target participated in First Amendment activities such as expressing opinions online, commenting in web forums and chat rooms, or posting or commenting on others' videos, such activities cannot serve as a basis for probable cause for a FISA warrant. Based on the discovery received and reviewed thus far, Jalil Aziz's online activity appears to be limited to such expressive behavior. Such expression clearly implicates First Amendment-protected conduct, no matter how repugnant that the government or even the general public may find it. *See Snyder v. Phelps*, 131 S. Ct. 1207 (2011) (First Amendment protects picketers at military funeral). Activities such as expressing support, urging others to express support, gathering information, and distributing information are protected and cannot serve as a basis

for probable cause. *See Nat'l Ass'n for Advancement of Colored People v. Button*, 371 U.S. 415, 444-45 (1963) (The "First Amendment protects expression and association without regard to the race, creed, or political or religious affiliation of the members of the group which invokes its shield, or to the truth, popularity, or social utility of the ideas and beliefs which are offered."). Moreover, the First Amendment includes the freedom to advocate the use of force or the violation of the law or even to advocate for unlawful action at some indefinite time in the future. *See Brandenburg v. Ohio*, 395 U.S. 444, 447-49 (1969); *Hess v. Indiana*, 414 U.S. 105, 108-09 (1973).

This, of course, begs the question whether there was any basis, other than protected First Amendment activity, for commencing FISA surveillance on Jalil Aziz. Should the answer be in the negative, the FISA surveillance would be invalid under §1805(a)(2)(A). In any event, it is paramount that the adversary process be allowed to function in its full capacity in this case to ensure the enforcement of FISA's First Amendment protections, and that defense counsel be allowed to view all FISA applications and warrants and fully participate in challenging their validity.

B. The FISA Applications May Contain Intentional or Reckless Falsehoods or Omissions In Contravention of Franks v. Delaware, 438 U.S. 154 (1978).

The Supreme Court's landmark decision in *Franks v. Delaware*, 438 U.S. 154 (1978) established the circumstances under which the target of a search may obtain an evidentiary hearing concerning the veracity of the information set forth in a search warrant affidavit. As the Court in *Franks* instructed, "where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statements are necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." *Franks*, 438 U.S. at 156-57.

The *Franks* opinion also sets a similar standard for suppression following the evidentiary hearing:

> in the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.

Id., at 156; *see United States v. Blackmon*, 273 F.3d 1204, 1208-10 (9th Cir. 2001) (applying *Franks* to Title III wiretap application); *United States v. Meling*, 47 F.3d 1546, 1553-56 (9th Cir. 1995) (same); *United States v. Duggan*, 743 F.2d 59, 77 n.6 (2d Cir. 1984) (suggesting that *Franks* applies

to FISA applications under Fourth and Fifth Amendments). See also *United States v. Hammond*. 351 F.3d 765, 770-71 (6th Cir. 2003) (applying *Franks* principles). The *Franks* principles apply to omissions as well as to false statements. See, e.g., *United States v. Carpenter*, 360 F.3d 591, 596-97 (6th Cir. 2004); *United States v. Atkin*, 107 F.3d 1213, 1216-17 (6th Cir.1997). Omissions will trigger suppression under *Franks* if they are deliberate or reckless, and if the search warrant affidavit, with omitted material added, would not have established probable cause.

As noted above, without the opportunity to review the applications, counsel cannot point to or identify any specific false statements or material omissions in those applications. Although that lack of access prevents counsel from making the showing that *Franks* ordinarily requires, counsel notes that the possibility that the government has submitted FISA applications with intentionally or recklessly false statements or material omissions is hardly speculative. For instance, in 2002, in *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620-21 (FISC 2002), rev'd on other grounds sub nom., *In re Sealed Case*, 310 F.3d 717 (FISCR 2002),[15] the FISC reported that beginning in March 2000, the Department of Justice (hereinafter "DOJ") had come "forward to confess

[15] The FISCR's 2002 decision in *In re Sealed Case* marked its first case since enactment of FISA in 1978.

error in some 75 FISA applications related to major terrorist attacks directed against the United States. The errors related to misstatements and omissions of material facts," including:

- "75 FISA applications related to major terrorist attacks directed against the United States" contained "misstatements and omissions of material facts." 218 F. Supp. 2d at 620-21;
- The government's failure to apprise the FISC of the existence and/or status of criminal investigations of the target(s) of FISA surveillance. *Id.*; and
- Improper contacts between criminal and intelligence investigators with respect to certain FISA applications. *Id.*

According to the FISC, "[i]n March of 2001, the government reported similar misstatements in another series of FISA applications . . ." *Id.* at 621. Nor were those problems isolated or resolved by those revelations. Instead, they proved persistent. A report issued March 8, 2006, by the DOJ Inspector General stated that the FBI found apparent violations of its own wiretapping and other intelligence-gathering procedures more than 100 times in the preceding two years, and problems appear to have grown more frequent in some crucial respects. *See* Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act, March

8, 2006 (hereinafter "DOJ IG Report"), available at http://www.usdoj.gov/oig/special/s0603/final.pdf.

The report characterized some violations as "significant," including wiretaps that were much broader in scope than authorized by a court ("over-collection"), and others that continued for weeks and months longer than authorized ("overruns"). *Id*. at 24-25.[16] FISA-related over-collection violations constituted 69% of the reported violations in 2005, an increase from 48% in 2004. See DOJ IG Report, at 29. The total percentage of FISA-related violations rose from 71% to 78% from 2004 to 2005, *Id*., at 29, although the amount of time "over-collection" and "overruns" were permitted to continue before the violations were recognized or corrected decreased from 2004 to 2005. *Id.* at 25.

Thus, a *Franks* hearing, and disclosure of the underlying FISA materials, are necessary in order to permit counsel the opportunity to prove that the affiants before the FISC intentionally or recklessly made materially false statements and omitted material information from the FISA applications.

[16] The DOJ Inspector General's report was not instigated by the government itself. Rather, the publication of documents released to Electronic Privacy Information Center (hereinafter "EPIC") in Freedom of Information Act litigation prompted the DOJ IG to use those and other documents as a basis for the report. In preparing the report the IG reviewed only those 108 instances in which the FBI itself reported violations to the Intelligence Oversight Board—a four-member Executive Branch body that ordinarily does not submit its reports to Congress.

C. The Collection of Foreign Intelligence Information Was Not a Significant Purpose of the FISA Surveillance.

It is difficult to see how tracking Jalil Aziz's online activity in Harrisburg, PA, including his frequent postings on message boards on popular websites visited by other Americans, involves foreign intelligence information, the collection of which being a significant purpose of any FISA surveillance. While individuals from overseas can also post on these messages boards and forums, such incidental and more often than not undisclosed international contacts and any foreign intelligence that could possibly be gleaned therefrom could not possibly serve as a significant purpose of the FISA surveillance. If such activity formed the basis for the foreign surveillance here, then the conclusion that Jalil Aziz's online activity was swept up by an NSA surveillance program, or E.O. 12333, would be unavoidable. Thus, the Court should order the government to disclose the FISA applications and related materials to the defense to allow the defense to provide input to the Court regarding these crucial determinations, including the impact of NSA surveillance.

D. The FISA Applications May Not Have Included the Required Certifications.

The Court should review the FISA applications to determine whether they contain all certifications required by §1804(a)(6). As the Ninth Circuit has declared in the Title III context, "[t]he procedural steps provided in the Act require 'strict

adherence,'" and "utmost scrutiny must be exercised to determine whether wiretap orders conform to [the statutory requirement]." *Blackmon*, 273 F.3d at 1207, quoting *United States v. Kalustian*, 529 F.2d 585, 588-9 (9th Cir.1975).

In addition, the Court should examine two certifications with particular care–(i) that the information sought is "the type of foreign intelligence information designated," and (ii) that the information "cannot reasonably be obtained by normal investigative techniques." *See* §1804(a)(6)(E). Particularly if the target of the wiretap is a "United States person" (such as Jalil Aziz), these two certifications must be measured by the "clearly erroneous" standard. *See* §1805(a)(4). As the Supreme Court has observed in relation to the similar provision in Title III, 18 U.S.C. § 2518(1)(e), "the necessity requirement 'exists in order to limit the use of wiretaps, which are highly intrusive.'" *Blackmon*, 273 F.3d at 1207, quoting *United States v. Bennett*, 219 F.3d 1117, 1121 (9th Cir. 2000) (internal quotation omitted). The necessity requirement "ensure[s] that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the [information sought]." *Id*.

The Court should also carefully examine the dates, in sequence, of all FISA orders in this case to determine whether there were any lapses of time during which wiretapping continued. The statutory scheme contemplates a seamless web: when a FISA order expires and the government wishes to continue the wiretap, the

expiring order must be replaced by an extension order, which, in turn, may be obtained only on the basis of a proper FISA application. *See* §1805(d)(1) & (2). FISA surveillance that continues past the expiration date of the FISA order that originally authorized it is just as unauthorized as a wiretap that is initiated without any FISA order at all. Should the Court order the government to disclose the FISA orders in this case to defense counsel, then counsel will be able to assist the Court in matching up all of the FISA orders by date—an arduous, albeit necessary, task.

E. The FISA Applications, and the FISA Surveillance, May Not Have Contained or Implemented the Requisite Minimization Procedures.

In order to obtain a valid FISA order, the government must include in its application a "statement of the proposed minimization procedures." §1804(a)(4). The purpose of these minimization procedures is to: (i) ensure that surveillance is reasonably designed to minimize the acquisition and retention of private information regarding people who are being wiretapped; (ii) prevent dissemination of non-foreign intelligence information; and (iii) prevent the disclosure, use, or retention of information for longer than seventy-two hours unless a longer period is approved by Court order. §1801(h).

As FISA involves particularly intrusive electronic surveillance—FISA interception is a "24/7" operation, as the Title III principle of "pertinence" is not applicable; instead, all conversations are captured, with minimization occurring

later and in other forms—minimization in the FISA context is critically important. A court and commentator have reasoned that "[i]n FISA the privacy rights of individuals are ensured not through mandatory disclosure [of FISA applications,] but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which normally governs law-enforcement surveillance." *United States v. Belfield*, 692 F.2d 141, 148 & n. 34 (D.C. Cir. 1982) (footnote omitted), quoting *Schwartz, Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs are Doing Their Job*, 12 RUTGERS L.J. 405, 408 (1981) (emphasis added). In order to determine whether there were adequate minimization procedures here, and that the government complied therewith, defense counsel should be provided with the FISA applications, orders, and related materials.

IV. The Government Must Provide Notice of the Surveillance Methods It Used.

Mr. Aziz is entitled to know how the government monitored his communications and activities, and then to test – through discovery and adversarial proceedings – whether the government lawfully obtained or derived the evidence it plans on using at trial from that surveillance. See generally *Keith*, 407 U.S. at 321; *Alderman*, 394 U.S. at 168. The sources of

authority requiring notice of the government's surveillance methods in criminal cases include, but are not limited to, the Fourth and Fifth Amendments to the Constitution, 18 U.S.C. § 3504, FISA itself (50 U.S.C. §§ 1806, 1881e) and Federal Rules of Criminal Procedure 12 and 16.[17]

Courts have long found notice a constitutionally required element of surreptitious searches, like wiretaps and sneak-and-peak entries. See, e.g., *Berger v. New York*, 388 U.S. 41, 60 (1967) (finding wiretapping statute unconstitutional because, among other things, it had "no requirement for notice as do conventional warrants"); *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (finding sneak-and-peak warrant constitutionally defective for its failure to provide explicitly for notice within a reasonable time); *United States v. Dalia*, 441 U.S. 238, 247-48 (1979) (observing that Title III provided a "constitutionally adequate substitute for advance notice by requiring that once the surveillance operation is completed the authorizing judge must cause notice to be served on those subjected to surveillance") (emphasis added). In response to these rulings, Congress has incorporated express notice provisions into many surveillance statutes, (see, e.g., 18 U.S.C. § 2518(8)(d) (Title III)), because it recognized that "all authorized

[17] The defense is, of course, willing to enter into a protective order or take other reasonable measures to accommodate legitimate security concerns that the government may have over the disclosure of this information. But those concerns do not trump Jalil Aziz's right to due process and to challenge the lawfulness of the surveillance techniques that the government used to obtain its evidence.

interceptions must eventually become known at least to the subject" in order to "insure the community that the techniques are reasonably employed." *United States v. Donovan*, 429 U.S. 413, 438 (1977) (quoting S. Rep. No. 1097, 90th Cong., 2d Sess., p. 2194 (1968)); see also 50 U.S.C. § 1806(c) (FISA electronic surveillance); *Id.* § 1825(d) (FISA physical search); *Id*. § 1842(c) (FISA pen register); *Cf.* Fed. R. Crim. P. 41(f) (requiring notice).

But courts can only confront the government's use of new technologies to carry out surreptitious searches in criminal investigations if the government provides notice, as it did in *Keith*, 407 U.S. 299-306. There, the government responded to the defendant's motion to compel the disclosure of electronic surveillance information in a national-security prosecution by publicly acknowledging that investigators had overheard the defendant's conversations using wiretaps. *Keith*, 407 U.S. at 299-300. Similarly, in *Kyllo v. United States*, 533 U.S. 27, 29-30 (2001), the defendant received notice that the government's search warrant application relied on evidence gathered using thermal-imaging technology. And in *United States v. Jones*, 132 S. Ct. 945, 948 (2011), the defendant had notice of the government's use of GPS tracking in order to record his movements. All of these seminal Fourth Amendment decisions would have been impossible if the defendants had not received notice of the government's secret and novel searches.

Due process entitles Mr. Aziz to test, on the facts of this case, whether the government's evidence should be suppressed as fruit of unlawful surveillance. Due process does not leave these questions to the government's sole judgment and discretion. *See Alderman*, 394 U.S. at 168 (recounting, in wiretapping challenge, Supreme Court's refusal to "accept the ex parte determination of relevance by the Department of Justice in lieu of adversary proceedings in the District Court"); *cf*., *e.g.*, *United States v. Eastman*, 465 F.2d 1057, 1062-63 & n.13 (3d Cir. 1972) (concluding that the Wiretap Act's statutory notice provision was "intended to provide the defendant whose telephone has been subject to wiretap an opportunity to test the validity of the wiretapping authorization"). Indeed, it would make little sense if the government could pre-determine, as part of its notice analysis, difficult or unique legal questions that a defendant would properly put before the Court – if only he knew.

Indeed, the Supreme Court has repeatedly made clear that when the government chooses to criminally prosecute someone, it may not keep the sources of its evidence secret:

> [T]he Government can invoke its evidentiary privileges only at the price of letting the defendant go free. The rationale of the criminal cases is that, since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense.

Jencks v. United States, 353 U.S. 657, 670-71 (1957) (quoting *United States v. Reynolds*, 345 U.S. 1, 12 (1953). Simply put, the government may not have it both ways – its secrecy and its prosecution – when an individual's liberty is at stake. Due process requires not only notice to a defendant, but may also call for disclosure of underlying surveillance applications or intercepts. This is why the Supreme Court has previously compelled the government to turn over records of wiretapped conversations in a national security case, even as the government threatened to abandon the prosecution if required to disclose them. *See Keith*, 407 U.S. at 318-24. The government is bound by that same choice here, wherever it has relied in whole or in part on undisclosed surveillance programs in the course of its investigation.

Therefore, the government must provide notice and discovery of the surveillance techniques that contributed to its investigation of Jalil Aziz, so that the Court may ultimately decide whether there is a legal and factual basis for suppression.

A. 18 U.S.C. § 3504 entitles Jalil Aziz to notice.

Congress has also provided a right to notice of electronic surveillance by statute. Under 18 U.S.C. § 3504, if a party in a proceeding before any court claims that "evidence is inadmissible" because "it is the primary product of an unlawful act or because it was obtained by the exploitation of any unlawful act" then the

government must "affirm or deny the occurrence of the alleged unlawful act." The statute defines "unlawful act" as "the use of any electronic, mechanical, or other device (as defined in section 2510(5) of this title) in violation of the Constitution or laws of the United States or any regulation or standard promulgated pursuant thereto." *Id*. § 3504(b).

Congress has provided that 18 U.S.C. § 3504 requires the "affirmance or denial of the fact of electronic surveillance, even if the government believes it was lawful." A "cognizable claim" for notice under the statute "need be no more than a 'mere assertion,' provided that it is a positive statement that illegal surveillance has taken place." *United States v. Apple*, 915 F.2d 899, 905 (4th Cir. 1990) (citing *United States v. Tucker*, 526 F.2d 279, 282 & n.4 (5th Cir. 1976). The party must make a prima facie showing that he was "aggrieved by the surveillance – i.e., "that [he] was a party to an intercepted communication, that the government's efforts were directed at [him], or that the intercepted communications took place on [his] premises." *Apple*, 915 F.2d at 905. Of course, because a defendant will have only limited information about the government's undisclosed surveillance, this initial showing need not be complete; it must only have a "colorable basis." Id. (citing *United States v. Pacella*, 622 F.2d 640, 643 (2d Cir. 1980)); *See also In re Grand Jury Matter*, 683 F.2d 66, 67 (3d Cir. 1982) (requiring notice under § 3504 upon the affidavits of the defendant and another individual that "there had

been 'unusual sounds' on the defendant's phone, . . . and that two policemen had told the other individual that the appellant's phone had been wiretapped").

Jalil Aziz qualifies for notice under § 3504. The government has collected information about him and his online activities using "other investigative tools" and obtained his private electronic communications through "other search warrants" while refusing to provide any specifics.

Accordingly, the government must provide notice of the surveillance methods used in this case and its purported legal authorities. *See United States v. Alter*, 482 F.2d 1016, 1027 (9th Cir. 1973) (finding the government's response to a claim under § 3504 insufficient because it was conclusory, failed to clearly identify all governmental agencies involved in the surveillance, failed to identify the date ranges of the surveillance, and relied on vague hearsay recitations).[18]

B. FISA requires notice and disclosure.

FISA expressly requires the government to provide a defendant with notice of some types of the surveillance at issue. *See* 50 U.S.C. §§ 1881e, 1806 (requiring notice of surveillance conducted under Sections 702 and 703). However, the government has a record of interpreting this requirement far too

[18] Although the government may argue that § 3504 is not applicable to FISA, it has been used before to secure notice of FISA surveillance. *See United States v. Hamide*, 914 F.2d 1147, 1149 (9th Cir. 1990).

narrowly, in order to avoid notifying criminal defendants of the surveillance used in their cases.

If the government used data obtained from Sections 702 and 703 in its investigation, it must give notice so that Jalil Aziz may seek to suppress any resulting evidence. Moreover, the government's determinations about whether its evidence is "derived from" this surveillance must be subjected to adversarial litigation and review. *See Alderman*, 394 U.S. at 183-84.

C. Rules 12 and 16 require notice and disclosure.

Federal Rules of Criminal Procedure 12(b)(3)(C) and 16(a)(1)(E)(i) also support Jalil Aziz's request for notice and discovery of the government's surveillance techniques because such information is necessary to prepare a motion to suppress. Indeed, Jalil Aziz's request falls squarely within Rule 16(a)(1)(E)(i)'s materiality requirement because a suppression motion directly implicates the government's ability to prove that he committed the crime charged. *See United States v. Armstrong*, 517 U.S. 456, 462 (1996) (holding that Rule 16(a)(1)(c), the predecessor to Rule 16(a)(1)(E)(i), applies to "shield" claims that "refute the Government's arguments that the defendant committed the crime charged"). Because Jalil Aziz cannot meaningfully respond to the evidence comprising the government's case in chief without knowing the extent of its surreptitious searches and seizures, he is entitled to notice and discovery.

Id. at 462 (defining the term "defense" in Rule 16 as the "defendant's response to the Government's case in chief").

V. The Underlying FISA Applications and Other Materials Should Be Disclosed to Defense Counsel to Enable Him to Assist the Court, and on Due Process Grounds.

A. Disclosure of FISA Materials to the Defense Pursuant to 50 §1806(f).

So that counsel may fully develop the arguments articulated above in order to allow the Court to make a fully informed decision regarding suppression and also as to other critical issues, such as the production of Brady material, the Court should order that the FISA applications and orders be disclosed to defense counsel. According to FISA's legislative history, disclosure may be "necessary" under §1806(f):

> where the court's initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as 'indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of non-foreign intelligence information, calling into question compliance with the minimization standards contained in the order.

United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982 [quoting S. Rep. No. 701, 95th Cong., 2d Sess. 64 (1979)]; *see, e.g., United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987) (same); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (same).

Here, as discussed above, there are ample justifications for disclosure of the FISA applications, which would permit defense counsel an opportunity to demonstrate that the requisite probable cause with respect to the issue of knowledge was lacking, that with respect to Jalil Aziz, a "United States person," the alleged "activities" fell within the protection of the First Amendment and, thus, could not be used as a basis for probable cause in any event, and/or that the information in the applications was either unreliable or obtained via illegal means. Disclosure would also afford defense counsel an opportunity to identify procedural irregularities.

Further, the Court can issue an appropriate Protective Order, to which Defendant's counsel would of course consent, that would provide elaborate protection for CLASSIFIED information, and which would permit CLASSIFIED materials to be disclosed to defense counsel but not to Defendant. *See* Classified Information Procedures Act (hereinafter "CIPA"), 18 U.S.C. App. III, at §3.

Thus, while no court in the more than twenty-five (25) year history of FISA has ordered disclosure of FISA applications, orders, or related materials, see, e.g., *In re Grand Jury Proceedings*, 347 F.3d 197, 203 (7th Cir. 2003) (citing cases); *United States v. Sattar*, 2003 U.S. Dist. LEXIS 16164, at *19 (S.D.N.Y. Sept. 15, 2003) (same), the circumstances herein compel

disclosure. Moreover, the existence of §1806(f) is an unambiguous declaration that Congress intended for courts to grant disclosure in appropriate cases. If §1806(f) is to be rendered meaningful at all, and not be rendered superfluous and entirely inert, it should apply in this case.

B. Disclosure of FISA Materials to the Defense Pursuant to §1806(g).

Even if the Court were to decline to find that disclosure of FISA-related materials to the defense is appropriate under §1806(f), the defense would still be entitled to disclosure of the FISA applications, orders, and related materials under §1806(g), which expressly incorporates the Fifth Amendment Due Process Clause, and provides that "[i]f the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." 50 U.S.C. §1806(g) (emphasis added). See also *United States v. Spanjol*, 720 F. Supp. 55, 57 (E.D. Pa. 1989) ("[u]nder FISA, defendants are permitted discovery of materials only to the extent required by due process. That has been interpreted as requiring production of materials mandated by [*Brady*], essentially exculpatory materials").

C. Scrubbing and Parallel Construction

In an effort to avoid suppression the government has taken to reverse engineering their prosecutions after they have used FISA or other avenues to gain

information. Notice and discovery is all the more necessary in light of government efforts to conceal surveillance through the use of "parallel construction." Parallel construction takes multiple forms, but is broadly designed to make evidence obtained from one source appear as though it was obtained from another.[19] Often, this involves reobtaining the same information using a second, less controversial method, in order to insulate the original method from judicial scrutiny.[20] Thus, emails initially obtained using a controversial foreign intelligence program might be reobtained using an ordinary Rule 41 warrant, leaving both the defendant and the court oblivious as to the original source. Unsurprisingly, parallel construction is routinely accompanied by instructions that agents shall not mention the original surveillance in any court filings, testimony, or legal proceedings.[21] In other

[19] *See, e.g., Sarah St. Vincent, Dispatches: US Surveillance Court Opinion Shows Harm to Rights,* Human Rights Watch (Apr. 22, 2016), http://tinyurl.com/hrw-parallel-construction (describing parallel construction as a process through which the government creates "an alternative explanation for how the authorities discovered a certain fact," thereby masking the true source of the information).

[20] See *John Shiffman & Kristina Cooke*, U.S. Directs Agents to Cover Up Program Used to Investigate Americans, Reuters (Aug. 5, 2013), http://reut.rs/1h07Hkl (describing parallel construction as a form of evidence laundering).

[21] *See* StellarWind IG Report at 401 (describing instructions forbidding agents from citing warrantless StellarWind surveillance "in affidavits, court proceedings, subpoenas, or for other legal or judicial purposes"); Jenna McLaughlin, *FBI Told Cops to Recreate Evidence from Secret Cell-Phone Trackers*, The Intercept (May 5, 2016), http://bit.ly/24uFSd5 (same for Stingray surveillance); Tim Cushing, *DEA Gets Unchecked Access to Call Records*, Techdirt (July 10, 2014), http://bit.ly/1ErIUAn (same for Hemisphere surveillance).

instances, agents have even withheld this information from prosecutors in order to avoid disclosure in court.[22]

The government cannot be allowed to avoid its notice and discovery obligations through so-called "parallel construction." The mere fact that the government may have later reobtained Jalil Aziz's communications using Rule 41 search warrants does not exempt the government from providing notice and discovery concerning its original searches. Accordingly, Jalil Aziz is entitled to challenge the lawfulness of those original searches in order to flesh out whether they tainted the Rule 41 search warrants.

Similarly, the Justice Department for years used so-called "scrubbing" procedures as part of a strategy to ensure that defendants never learned of warrantless wiretapping conducted under the "StellarWind" program and thus had no opportunity to challenge it.[23] And the government has recently taken the position that defendants have no right to know when the NSA's bulk call- records program contributed to prosecutions – even though that surveillance program was declared illegal by the Second Circuit after its existence was finally revealed. *See*

---

[22] *See* Shiffman & Cooke, *supra*; Brad Heath, *FBI Warned Agents Not to Share Tech Secrets with Prosecutors*, USA Today (Apr. 20, 2016), http://usat.ly/1W2zIvl.

[23] *See* DOJ Office of the Inspector General, *A Review of the Department of Justice's Involvement with the President's Surveillance Program* (July 2009), http://nyti.ms/1Yvwvop (PDF pages 415–25, 672–77, 694–96) (hereinafter "StellarWind IG Report").

Gov't Resp. Br. at 71, *United States v. Moalin*, No. 13-50572 (9th Cir. Apr. 15, 2016 (ECF No. 34-1); *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015). In short, the government has repeatedly hidden its most intrusive and controversial surveillance methods from criminal defendants, in order to thwart any adversarial legal challenge. Such obfuscation should not be allowed to undermine the fair trial guaranteed to Jalil Aziz by the United States Constitution.

D. Ex Parte Proceedings Are Antithetical to the Adversary System of Justice.

Lack of disclosure would render the proceedings on the validity of the FISA surveillance ex parte, as the challenges on Jalil Aziz's behalf would be made without access to documents and information essential to the determination of his motion. Such proceedings are antithetical to the adversary system that is the hallmark of American criminal justice. *Ex parte* proceedings impair the integrity of the adversary process and the criminal justice system. As the Supreme Court has recognized, "'[f]airness can rarely be obtained by a secret, one-sided determination of facts decisive of rights. . . . No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it.'" *United States v. James Daniel Good Real Property, et. al.*, 510 U.S. 43, at 55 (1993) (quoting *Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123, 170-72 (1951) (Frankfurter, J., concurring). *See also United States v. Madori*, 419 F.3d 159, 171 (2d Cir. 2005), citing *United States v.*

Arroyo-Angulo, 580 F.2d 1137, 1145 (2d Cir.1977) (closed proceedings "are fraught with the potential of abuse and, absent compelling necessity, must be avoided") (other citations omitted).

In *United States v. Abuhamra*, 389 F.3d 309 (2d Cir. 2004), the Second Circuit reemphasized the importance of open, adversary proceedings, declaring that "[p]articularly where liberty is at stake, due process demands that the individual and the government each be afforded the opportunity not only to advance their respective positions but to correct or contradict arguments or evidence offered by the other." *Abuhamra*, 389 F.3d at 322-23 [citing *McGrath*, 341 U.S. at 171 n. 17] (Frankfurter, J., concurring), noted that there is a "duty lying upon everyone who decides anything to act in good faith and fairly listen to both sides . . . always giving a fair opportunity to those who are parties in the controversy for correcting or contradicting any relevant statement prejudicial to their view") (citation and internal quotation marks omitted).

As the Ninth Circuit observed in the closely analogous context of a secret evidence case, "[o]ne would be hard pressed to design a procedure more likely to result in erroneous deprivations. . . . [T]he very foundation of the adversary process assumes that use of undisclosed information will violate due process because of the risk of error." *American-Arab Anti-Discrimination Committee v. Reno*, 70 F.3d

1045, 1069 (9th Cir. 1995) (quote marks omitted); *Kiareldeen v. Reno*, 71 F. Supp. 2d 402, 412-14 (D. N.J. 1999) (same).

Similarly, in the Fourth Amendment context, including in relationship to electronic surveillance, the Supreme Court has twice rejected the use of *ex parte* proceedings on grounds that apply equally here. In *Alderman v. United States*, 394 U.S. 165 (1969), the Court addressed the procedures to be followed in determining whether government eavesdropping in violation of the Fourth Amendment contributed to the prosecution case against the defendants. The Court rejected the government's suggestion that the district court make that determination in camera and/or ex parte. The Court observed:

> [a]n apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused's life. And yet that information may be wholly colorless and devoid of meaning to one less well acquainted with all relevant circumstances.

Id. at 182. And in ordering disclosure of improperly recorded conversations, the Court declared:

> [a]dversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny that the Fourth Amendment exclusionary rule demands.

Id. at 184.

Likewise, the Supreme Court held in *Franks*, that a defendant, upon a preliminary showing of an intentional or reckless material falsehood in an affidavit underlying a search warrant, must be permitted to attack the veracity of that affidavit. The Court rested its decision in significant part on the inherent inadequacies of the ex parte nature of the procedure for issuing a search warrant, and the contrasting enhanced value of adversarial proceedings:

> [T]he hearing before the magistrate [when the warrant is issued] will not always suffice to discourage lawless or reckless misconduct. The pre-search proceeding is necessarily ex parte, since the subject of the search cannot be tipped off to the application for a warrant lest he destroy or remove evidence. The usual reliance of our legal system on adversary proceedings itself should be an indication that an ex parte inquiry is likely to be less vigorous. The magistrate has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations. The pre-search proceeding will frequently be marked by haste, because of the understandable desire to act before the evidence disappears; this urgency will not always permit the magistrate to make an independent examination of the affiant or other witnesses.

438 U.S. at 169.

The same considerations that the Supreme Court found compelling in *Alderman* and *Franks* militate against ex parte procedures in the FISA context. Indeed, the lack of any authentic adversary proceedings in FISA litigation more than likely accounts for the government's perfect record in defending FISA and

FISA-generated evidence. After all, denying an adversary access to the facts constitutes an advantage as powerful and insurmountable as exists in litigation.

As the FISC itself has acknowledged, for example, without adversarial proceedings, systemic executive branch misconduct—including submission of FISA applications with "erroneous statements" and "omissions of material facts"—went entirely undetected by the courts until the FISC directed that the Department of Justice review FISA applications and submit a report to the FISC. *See In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp.2d at 620-21, rev'd on other grounds, 310 F.3d 717 (FISCR 2002).

However, as discussed above, the complete deference now required of the courts toward the executive with respect to FISA renders any such "in-depth oversight" and "expanded conception of minimization" (relied upon in *Belfield* 692 F.2d at 148 & n. 34) entirely illusory. As a result, §§1806(f) & (g), and the disclosure they authorize, assume significantly greater meaning and importance in evaluating the validity of FISA applications. Also, defense counsel can acquire the requisite security clearances to view the material, thereby further eliminating any justification for non-disclosure, or any claim that such limited, safe disclosure presents any danger to national security.

Lastly, the Court's review in camera is not a substitute for defense counsel's participation. As the Supreme Court recognized in *Alderman* "[i]n our adversary system, it is enough for judges to judge. The determination of what may be useful to the defense can properly and effectively be made only by an advocate." 394 U.S. at 184.[24] Accordingly, either under §1806(f), §1806(g), and/or the Due Process clause, disclosure of the FISA materials is authorized and appropriate in this case.

V. Whether or Not the Court Orders Disclosure so that Counsel May Meaningfully Participate in the Motion to Suppress, this Court's Review of the FISA Warrant or Warrants is De Novo.

This Court should review the FISA applications and orders de novo. *United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004) (noting district court's de novo review and conducting its own de novo review of FISA materials), vacated on other grounds, 543 U.S. 1097 (2005); *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000) (same); *see also United States v. Campa*, 529 F.3d 980,

[24] As the District Court in *United States v. Marzook*, 412 F. Supp.2d 913 (N.D. Ill. 2006), explained in the context of deciding whether to close a suppression hearing to the public because of the potential revelation of classified information thereat,

> [i]t is a matter of conjecture whether the court performs any real judicial function when it reviews classified documents in camera. Without the illumination provided by adversarial challenge and with no expertness in the field of national security, the court has no basis on which to test the accuracy of the government's claims.

Id., at 921, quoting *Stein v. Department of Justice & Federal Bureau of Investigation*, 662 F.2d 1245, 1259 (7th Cir. 1981)

991 (11th Cir. 2008); *United States v. Kashmiri*, 2010 U.S. Dist. LEXIS 119470, *4 (N.D. Ill. Nov. 10, 2010) ("The court conducts a de novo review of the FISA materials to determine if the electronic surveillance authorization was based upon appropriate probable cause.")

Courts have held that a reviewing court is to conduct essentially the same review of the FISA application and associated materials that the FISC conducted upon receiving an application requesting a FISA order. *See, e.g., In re Grand Jury Proceedings of Special April 2002 Grand Jury*, 347 F.3d 197, 204-05 (7th Cir. 2003). Accordingly, the court reviews, first, the adequacy of the FISA materials at issue "de novo with no deference accorded to the FISC's probable cause determinations," and second, the Executive Branch's certifications, which are reviewed for clear error. *United States v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006).

Robust de novo review is all the more important if meaningful defense participation in the suppression motion is not permitted, and the government's assertions could thus be untested by the adversarial process. Moreover, there is reason for this Court's review to be more exacting than the FISC's review of the government's applications for a FISA order. Unlike the FISC applications, the FISA activity is no longer about intelligence gathering, but is now being used to seek a conviction and imprisonment of a United States citizen. The focus should

therefore now be on the rights of Jalil Aziz, rather than simply general interests in intelligence gathering.

The Court should also be cognizant of its role as a neutral and detached arbiter, and the distinct separation of powers at issue here. The role of a FISC judge is significantly different than that of an ordinary judge or magistrate because the statute directs deference to the Executive Branch's certifications and also because the FISA applications and orders are shrouded in almost complete secrecy.

VI. Should the Court not Allow Defense Counsel's Participation Regarding FISA Searches and Seizures, the Court Should Also Consider Potential FISA's Constitutional Violations, both Facially and as Applied in this Case.

Review of the issues raised by Jalil Aziz's motion to suppress and for disclosure requires the Court to engage in interpretation and construction of a number of provisions of FISA. At a minimum, the provisions detailed below are necessarily called into question. To the extent the government disagrees with counsel's interpretations of those provisions, or the Court is inclined to side with some of the Circuits that have read the statute more broadly, review in this case will require consideration of the constitutionality of the statute itself. There are a number of reasons why a broad reading of FISA, particularly as amended by the Patriot Act, could be said to violate the First, Fourth, Fifth, and Sixth Amendments. As in all cases, the Court's review should proceed under the basic

rule of statutory construction that where a plausible reading of a statute would avoid serious constitutional problems, the Court should follow that construction instead of a construction that raises serious constitutional issues. *See Skilling v. United States*, 130 S.Ct. 2896, 2940 (2010). To the extent the Court does not narrowly read the FISA statute, the procedures it purports to authorize should be found to violate the Constitution. Moreover, the constitutionality of FISA should be viewed as applied to this case.

Prior to the enactment of FISA, and for the first twenty-five (25) years of its existence, the "primary purpose" for surveillance or searches was required to be intelligence gathering with respect to a "foreign power" or an "agent of a foreign power." *United States v. Truong Dinh Hung*, 629 F.2d 908, 912-13 (4th Cir. 1980); 50 U.S.C. § 1805(a)(3) (2000). The non-criminal purpose standard was essential to the cases upholding FISA's constitutionality. Courts refined the statutory standard and held that FISA-generated evidence was admissible so long as the government's "primary purpose" in conducting the electronic surveillance was the gathering of foreign intelligence information—as opposed to information to build a criminal investigation of the target of the eavesdropping or search. *See, e.g., United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984). The facts of the charges against Jalil Aziz show that the primary purpose was for criminal prosecution.

However, in October 2001, through the Patriot Act, Congress—without any debate—amended the language of FISA and changed the language requiring that "the purpose" of the search or surveillance to be the acquisition of foreign intelligence information, to requiring that such acquisition be "a significant purpose." 50 U.S.C. § 1804(a)(7)(B) and § 1823(a)(7)(B) (as amended by Pub.L. 107-56, Title II, § 218, Oct. 26, 2001) (emphasis added). *See also In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611 (FISA 2002), reversed in part, *In re Sealed Case*, 310 F.3d 717 (FISA Rev. 2003). These Patriot Act amendments dramatically expanded the class of investigations in which FISA is available to the government, and have enabled the government to conduct surveillance to gather evidence for use in a criminal case without a traditional warrant—so long as the government can state that there is a "significant purpose" in gathering foreign intelligence. Thus, while FISA set out to reduce the probable cause requirement only for national security intelligence gathering, a consequence —intended or not—of the Patriot Act has been that the Executive Branch may now "bypass the Fourth Amendment" to gather evidence for a criminal prosecution. *See Mayfield v. United States*, 504 F. Supp. 2d 1023, 1036-37 (D. Ore. 2007) (holding FISA as amended to be unconstitutional), vacated and remanded on other grounds, 599 F.3d 964 (9th Cir. 2010) (plaintiff lacked standing due to settlement agreement with government).

While courts have found that the reduced "significant purpose" standard does not violate the Constitution, there has been no such ruling after the recent widely publicized public disclosures regarding the expansive nature of the NSA PRISM program, STINGRAY intercepts and the like—particularly insofar as they involve the collection of domestic communications of American citizens. This is significant due to the history of FISA and the approval of the "significant purpose" standard based on the rationale that the purpose—whether significant or primary—was still the gathering of foreign intelligence regarding a foreign power or agent of a foreign power. *See, e.g., United States v. Pelton*, 835 F.2d 1067, 1075- 76 (4th Cir. 1987); *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987).[25]

The fact we now know that NSA surveillance programs essentially vacuum up an untold number of domestic communications calls into question the very underpinnings of such prior decisions. No longer can it simply be naively accepted that the purpose of FISA surveillance is foreign intelligence, especially in a case

[25] *See also See also United States v. Brown*, 484 F.2d 418, 427 (5th Cir. 1973) ("The serious step of recognizing the legality of a wiretap can be justified only when, as in the case before us, the foreign and sensitive nature of the government surveillance is crystal clear.") (Goldberg, J., concurring); *United States v. Butenko*, 494 F.2d 593, 606 (3d Cir. 1974) ("Since the primary purpose of these searches is to secure foreign intelligence information, a judge, when reviewing a particular search must, above all, be assured that this was in fact its primary purpose and that the accumulation of evidence of criminal activity was incidental."); *United States v. Buck*, 648 F.2d 871 (9th Cir. 1977); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (affirming denial of motion to suppress, but only upon express finding that purpose of the surveillance was foreign intelligence gathering and was not "directed towards criminal investigation or the institution of a criminal prosecution."), abrogated by statute on other grounds, 630 F.3d 102 (2d Cir. 2010).

like this, where it strains credulity to see how web postings on websites involved foreign intelligence—no matter how disagreeable the government may find the content of those postings.

In *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972), the Court rejected the government's contentions that national security investigations are too complex for judicial evaluation, and that requiring prior judicial approval would fracture secrecy essential to official intelligence gathering. Id. at 318-21. The Supreme Court also rejected the government's argument that exceptions to the Fourth Amendment warrant requirement should be recognized for domestic security surveillance. *Id*. at 316-17. The Supreme Court further warned that "[t]he historical judgment, which the Fourth Amendment accepts, is that un-reviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." *Id*. at 316-17. See also *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) (stating that "the investigation of criminal activity cannot be the primary purpose of the surveillance," and that FISA may "not be used as an end-run around the Fourth Amendment's prohibition of warrantless searches"). The Supreme Court's warning now seems prescient.

It appears now that through the virtually unchecked NSA surveillance programs, that until recently operated in near secrecy, the government has—under

the auspices of FISA and more likely the FAA or E.O. 12, 333—engaged in the domestic surveillance forbidden by *Keith* and traditional First and Fourth Amendment jurisprudence. If the government used FISA, E.O. 12, 333, or the FAA in such a manner in this case, then the Court should find its application unconstitutional and suppress any and all evidence obtained as a result of such surveillance. Any evidence collected as a result of those constitutional violations should be suppressed as fruit of the poisonous tree and excluded from the prosecution of Jalil Aziz.

This case presents a historical opportunity for the Judicial Branch to exercise its time honored authority to put a stop to unfettered and unconstitutional Executive Branch covert activity—the very activity FISA was designed to correct in light of the Church Committee intelligence scandals which seem almost quaint when compared to the scope of these current covert operations. There is a slippery slope between Jalil Aziz and every other American citizen with a cell phone.

WHEREFORE, Jalil Aziz asks This Honorable Court to enforce the Constitution by ordering all the notice and discovery which would be available in a regular, fair criminal trial or suppress all evidence gathered through "secret" or "confidential" means.

Respectfully submitted,

/s/ Thomas A. Thornton
Thomas A. Thornton, Esquire
Attorney ID# 44208
Federal Public Defender's Office
100 Chestnut Street, Suite 306
Harrisburg, PA 17101
Tel. No. 717-782-2237
Fax No. 717-782-3881
tom_thornton@fd.org
Attorney for Jalil Ibn Ameer Aziz